IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
FT. WAYNE DIVISION

RORY HILL, NICOLE HILL, and DAWN McLAUGHLIN, individuals, on behalf of themselves and all others similarly situated, Plaintiffs, vs. MEDICAL INFORMATICS ENGINEERING, INC., Defendant.	Case No. 1:15-cv-00204 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Rory Hill, Nicole Hill, and Dawn McLaughlin ("Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Class Action Complaint ("Complaint") against Defendant Medical Informatics Engineering, Inc. ("MIE" or "Defendant") for its unlawful and deceptive failure to properly safeguard personally-identifiable information ("PII") entrusted to it, including names, dates of birth, telephone numbers, street addresses and personal health information ("PHI"). Further, other data may be affected including social security numbers, account numbers, and health insurance policy information.

2. MIE states the following about its business:

> "Medical Informatics Engineering has a long history in interoperable healthcare data exchange, starting with the development of one of the earliest sustainable HIEs. The Med-Web, a secure, web-based, private communication network enabling healthcare providers to transmit and share electronic information, fueled adoption or electronic health records at a local rate ten times the national average, and continues to support northeast Indiana physicians today."[1]

Its system interfaces with the following: billing and practice management systems, labs and pharmacies, HR and other employer-based enterprise software, physician and hospital systems, registries and state designated HIEs, and patient portals.

3. On May 26, 2015, MIE discovered suspicious activity related to one of its servers. Forensic investigation indicates the unauthorized access began on May 7, 2015.

4. On July 17, 2015, when the data breach was disclosed by written correspondence, the investigation had been ongoing for over two months. Other than confirming the data breach, MIE has not provided any information as to the extent of this compromise, how the attackers were able to access its system, if any measures have been taken to prevent further breaches or whether the vulnerability of its database warehouses has been contained. In fact, Chief Operating Officer, Eric Jones, said in a telephone interview that the number of affected patients has not been determined, and declined to speculate how many there might be.[2]

PARTIES

[1] http://www.mieweb.com/company

[2] http://www.indystar.com/story/news/crime/2015/06/10/st-francis-affected-hacking-medical-software-company/71028528/

5. Plaintiffs Rory Hill and Nicole Hill are natural persons and residents of the State of Indiana.

6. Plaintiff Dawn McLaughlin is a natural person and a resident of the State of Indiana.

7. Headquartered in Fort Wayne, Indiana, Defendant Medical Informatics Engineering, Inc. is an Indiana corporation located at 6302 Constitution Drive, Ft. Wayne, Indiana 46804.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

9. This Court has personal jurisdiction over Defendant because it conducts significant business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

10. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiffs' Complaint occurred in this District.

FACTUAL BACKGROUND

11. MIE was formed October 23, 1995.

12. On May 7, 2015, attackers gained unauthorized access to MIE's system. Mr. Jones wrote the Plaintiffs on or about July 17, 2015, and indicated the following:

> "On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your personal and protected health information."

13. MIE discovered the attack some time during the week of May 26, 2015, and investigators are still evidently determining the extent of the incursion.

14. The company has indicated that personal medical data has been compromised, additionally the following types of information were stolen in the breach — including names, birth dates, social security numbers, addresses, insurance information — could represent a treasure trove to cyber-thieves.

The Worst Kind of Data Breach and It Could Have Been Prevented

15. Numerous tools exist that companies can deploy and this episode brings home the need for better protective measures. Benn Konsynski, George S. Craft professor of information systems and operations management at Emory University's Goizueta Business School stated the following in the wake of the Anthem data breach: "The scale is enormous. I am sort of bewildered that we still have this magnitude of exposure," he said. "It certainly is the third or the fourth wake-up call to the market. ... (It) is incumbent on firms like that to go the extra mile to make

sure that exposure is prevented or minimized in those processes."[3] After the Anthem data breach, companies were on notice as to the magnitude of the threat.

The MIE Breach Has Caused Its Members Severe, Long Term Effects

16. According to security experts, the type of information that the hackers have accessed from MIE's systems could create problems for those affected for years to come.

17. Privacy expert Rick Kam, president and co-founder of the Portland, Oregon-based company ID Experts, says: "Such information can be sold on the black market to open the door to a range of identity theft schemes. For instance, criminals have all the information they need to submit fraudulent tax returns[.]" Victims might not realize they have been affected until they try to process their returns.[4]

18. Or, a person could use the information to engage in medical identity fraud, said Ann Patterson, senior vice president and program director of the Medical Identity Fraud Alliance. Consumers need to carefully review all explanations of benefits they received from insurers to make sure that they have not been the victim of medical identity theft. Medical identity theft could inadvertently result in harm to the victim, Patterson added. For instance, if the perpetrator does not share the same blood type as the victim, a person could receive a dangerous transfusion.[5]

---

[3] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battle-customers/22953623/

[4] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battle-customers/22953623/

[5] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battle-customers/22953623/

19. According to Stu Sjouwerman, CEO of Clearwater, Florida-based security firm KnowBe4, the records breached are especially valuable to criminals. "In the underground cyber market, healthcare records can bring $50 each and up. Compare that to credit card records, which generally bring only a dollar or two each."[6]

20. On July 23, 2015, MIE posted such a warning on its website.[7]

CLASS ALLEGATIONS

21. Plaintiffs Rory Hill, Nicole Hill, and Dawn McLaughlin bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and a Class of similarly situated individuals, defined as:

> All persons in the United States whose personally identifiable information, personal financial information or personal health information was compromised as a result of the data breach first disclosed by Medical Informatics Engineering on July 17, 2015.

Excluded from the Class are: (1) any Judge presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) counsel for Plaintiff and Defendant; (4) persons who properly execute and file a timely request for exclusion from the class; (5) the legal representatives, successors or assigns of any such excluded persons; (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against

[6] http://www.enterprise-security-today.com/news/Anthem-Hit-with-Huge-Data-Breach/story.xhtml?story_id=012000EWITUO#

[7] http://www.mieweb.com/notice

Defendant; and (7) any individual who contributed to the unauthorized access of Defendant's database.

22. **Numerosity**: The exact number of the members of the Class is unknown to Plaintiffs at this time, but on information and belief, there are over 100 people in the Class, making joinder of each individual member impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

23. **Typicality**: Plaintiffs' claims are typical of the claims of all the other members of the Class. Plaintiffs and the Class members sustained substantially similar damages as a result of Defendant's uniform wrongful conduct, based upon the same transactions that were made uniformly with Plaintiffs and the public.

24. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

25. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of

the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

26. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

(a) Whether MIE failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' PII;

(b) Whether MIE properly implemented its purported security measures to protect Plaintiffs' and Class members' PII from unauthorized access, dissemination and misuse;

(c) Whether MIE's conduct was negligent?

(d) Whether Plaintiffs and Class members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

27. **Policies Generally Applicable to the Class**: MIE has acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

28. Plaintiffs reserve the right to revise the definitions of the Class based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION

Negligence
(On Behalf of Plaintiffs and the Class)

29. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

30. MIE owed a duty to Plaintiffs and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing MIE's security systems to ensure that Plaintiffs' and Class members' PII and PHI in MIE's possession was adequately secured and protected. MIE further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

31. MIE owed a duty to Plaintiffs and members of the Class to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII and PHI of Plaintiffs and members of the Class.

32. MIE owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate security practices. MIE inadequately safeguarded such information on its computer systems. MIE knew that a breach of its systems would cause damages to Plaintiffs and members of the Class and MIE had a duty, which it assumed, to adequately protect such sensitive financial and personal information.

33. Plaintiffs and members of the Class entrusted MIE with their PII and PHI and MIE assumed the duty to safeguard their information, and MIE was in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the MIE data breach.

34. MIE knew, or should have known, of the risks inherent in collecting and storing the PII and PHI Plaintiffs and members of the Class who trusted MIE to provide adequate security of that information.

35. MIE's own conduct also created a foreseeable risk of harm to Plaintiffs and members of the Class. MIE's misconduct included, but was not limited to, (a) its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein; (b) its decision not to comply with industry standards for the safekeeping and maintenance of the PII and PHI of Plaintiffs and Class members; (c) its

failure to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII and PHI of Plaintiffs and members of the Class; (d) its failure to properly implement technical systems or security practices that could have prevented the loss of the data at issue; and (e) its failure to properly maintain Plaintiffs' and the Class members' sensitive PII and PHI.

36. Given the risk involved and the amount of data at issue, MIE's breach of its duties was entirely unreasonable.

37. MIE breached its duties to timely and accurately disclose that Plaintiffs' and Class members' PII and PHI in MIE's possession had been or was reasonably believed to have been, stolen or compromised.

38. MIE knew that Plaintiffs and members of the Class were foreseeable victims of a data breach of its systems because of laws and statutes that require MIE to reasonably safeguard and implement policies and procedures to protect unsecured "electronic protected health information" including the Class members PII and PHI.

39. But for MIE's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, their PII and PHI would not have been compromised.

40. The injury and harm suffered by Plaintiffs and members of the Class as set forth above was the reasonably foreseeable result of MIE's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI within MIE's possession. MIE knew or should have known that its sys-

tems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and Class members' personal and financial information were inadequate and vulnerable to being breached by hackers.

41. Plaintiffs and members of the Class suffered injuries and losses described herein as a direct and proximate result of MIE's conduct resulting in the data breach, including MIE's lack of adequate reasonable and industry-standard security measures. Had MIE implemented such adequate and reasonable security measures, Plaintiffs and Class members would not have suffered the injuries alleged, as the MIE data breach would likely have not occurred.

42. A special relationship exists between Plaintiffs and members of the Class and MIE.

43. Holding MIE accountable for its negligence will further the policies underlying negligence law and will require MIE and encourage similar companies that obtain and retain sensitive consumer PII and PHI to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such health care member information.

44. As a direct and proximate result of MIE's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Rory Hill, Nicole Hill, and Dawn McLaughlin individually and on behalf of the Class, prays for the following relief:

A. Certification of this case as a class action on behalf of the Class defined above, appointment of Rory Hill, Nicole Hill and Dawn McLaughlin as Class representative, and appointment of their counsel as Class counsel;

B. Injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the members of the Class, including, *inter alia*: (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; and (ii) requiring Defendant to protect all data collected through the course of its business in accordance with industry and other applicable standards;

C. An award of appropriate damages to Plaintiffs and the Class in an amount to be determined at trial;

D. An award to Plaintiffs and the Class of their reasonable litigation expenses and attorneys' fees;

E. An award to Plaintiffs and the Class of pre- and post-judgment interest, to the extent allowable; and

F. An award of such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

Dated: August 4, 2015

PRICE WAICUKAUSKI & RILEY, LLC

/s/ William N. Riley

William R. Riley (#14941-49)
Joseph N. Williams (#25847-49)
James A. Piatt (#28320-49)
301 Massachusetts Avenue
Indianapolis, IN 46204
Telephone: (317) 633-8787
Facsimile: (317) 633-8797
wriley@price-law.com
jwilliams@price-law.com
jpiatt@price-law.com

Counsel for Plaintiffs, Rory Hill, Nicole Hill and Dawn McLaughlin